HALF-DAY WORKSHOP ON
PERSONAL DATA PROTECTION LAW

Meeting Room level 2 | Ahmad Ibrahim Kulliyyah of Laws | IIUM Gombak | Wednesday, 28th May 2014 | 09.00 am - 01.00 pm

Brought by:
Civil Law Department | Ahmad Ibrahim Kulliyyah of Laws | International Islamic University Malaysia

SPEAKERS:

Dr. Federico Feretti
Brunel University, London

Mr. Noriswadi Ismail
Quotient Consulting, KL

Dr. Sonny Zulhuda
AIKOL, International Islamic University Malaysia

HIGHLIGHTS:

- Understanding Key Features of PDP Act 2010:
- What it means for University, Staff and Students
- Implementing PDP Law in Educational Sector
- Basic Roadmap for Privacy Compliance
- Teaching Data Protection in Law Schools
- Lessons from the UK & Europe

PDP LAW AND THE UNIVERSITY DATA ECOSYSTEM: UNDERSTANDING THE CONTEXT

Dr. Sonny Zulhuda

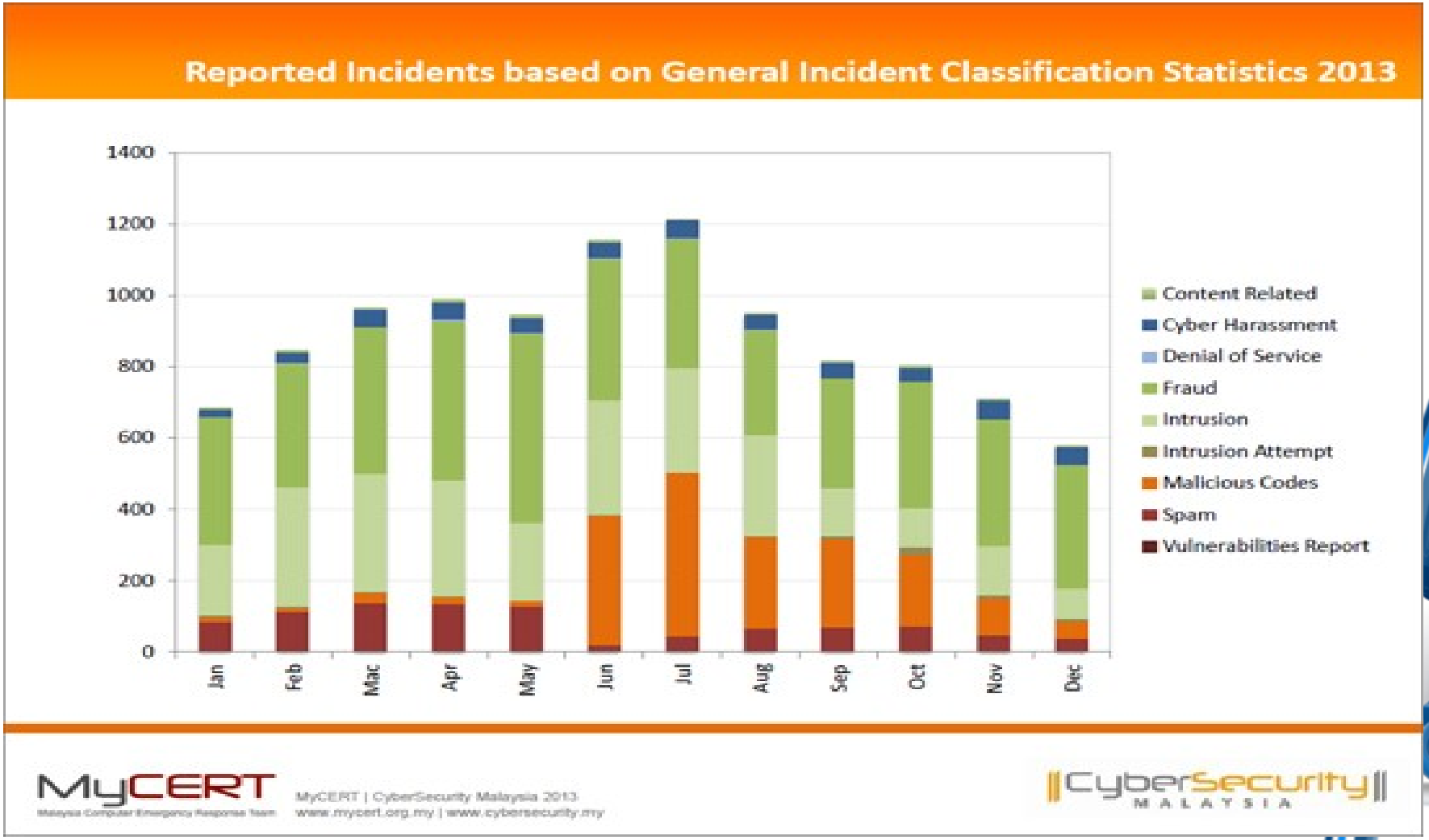
International Islamic University Malaysia

HALF-DAY WORKSHOP ON PDP LAW

Ahmad Ibrahim Kulliyyah of Laws (AIKOL), IIUM

28 May 2014

Data Breach in Malaysia (2013)



Illegal to sell personal data

> Public to have more control over their own particulars under Personal Data Protection Act

BY ***ALYAA ALHADJRI*** AND ***DOROTHY CHENG***
newsdesk@thesundaily.com

KUALA LUMPUR: The Personal Data Protection Act 2010 to be enforced in January will make it illegal for corporate entities or individuals to sell personal information or allow the use of data by third parties.

Deputy Information, Communications and Culture Minister Datuk Joseph Salang said a conviction under the act will impose a fine not exceeding RM300,000 or imprisonment not exceeding two years, or both.

"A Personal Data Protection Department had been established by the ministry in May last year, with a mandate to enforce the law, and increase consumer confidence in commercial transactions," he said in his speech at the 2nd Annual Personal Data Protection Summit yesterday.

He said 3,889 cybercrime and online shopping fraud cases had been reported between January and September this year.

"Online shopping fraud registered losses of almost RM14.6 million while cybercrimes totalled RM80.2 million during the same period," he said, noting that banking fraud incidents topped the list of cybercrimes.

With enforcement of the law, Joseph said the public will have more control over their personal

Data Breach Cases in Malaysia

GEORGE TOWN: Court held doctor liable for unauthorized capture of his patient's **private parts photographs** during a surgery (2010)

KUALA TERENGGANU: A telco operator was sued for negligence over a leak of phone and SMS **communications data** (2010),

KOTA KINABALU: A former beauty queen sued a company for using her **photograph** in their product packaging & in a billboard (2011)

LABUAN: Court issued injunction to stop a former employee marketing staff from disclosing **customers' data** to new employer (2010)

SANDAKAN: court held a credit report agency liable for its **inaccurate credit reporting** supplied to banks (2011)

KUALA LUMPUR: High Court ordered a medical centre to pay a total of RM400,000 to a community leader for revealing his **psychiatric medical records** (2013)

KL & SELANGOR: Schools who fixed **CCTV in their toilets** were told to remove it due to privacy concern (2013)

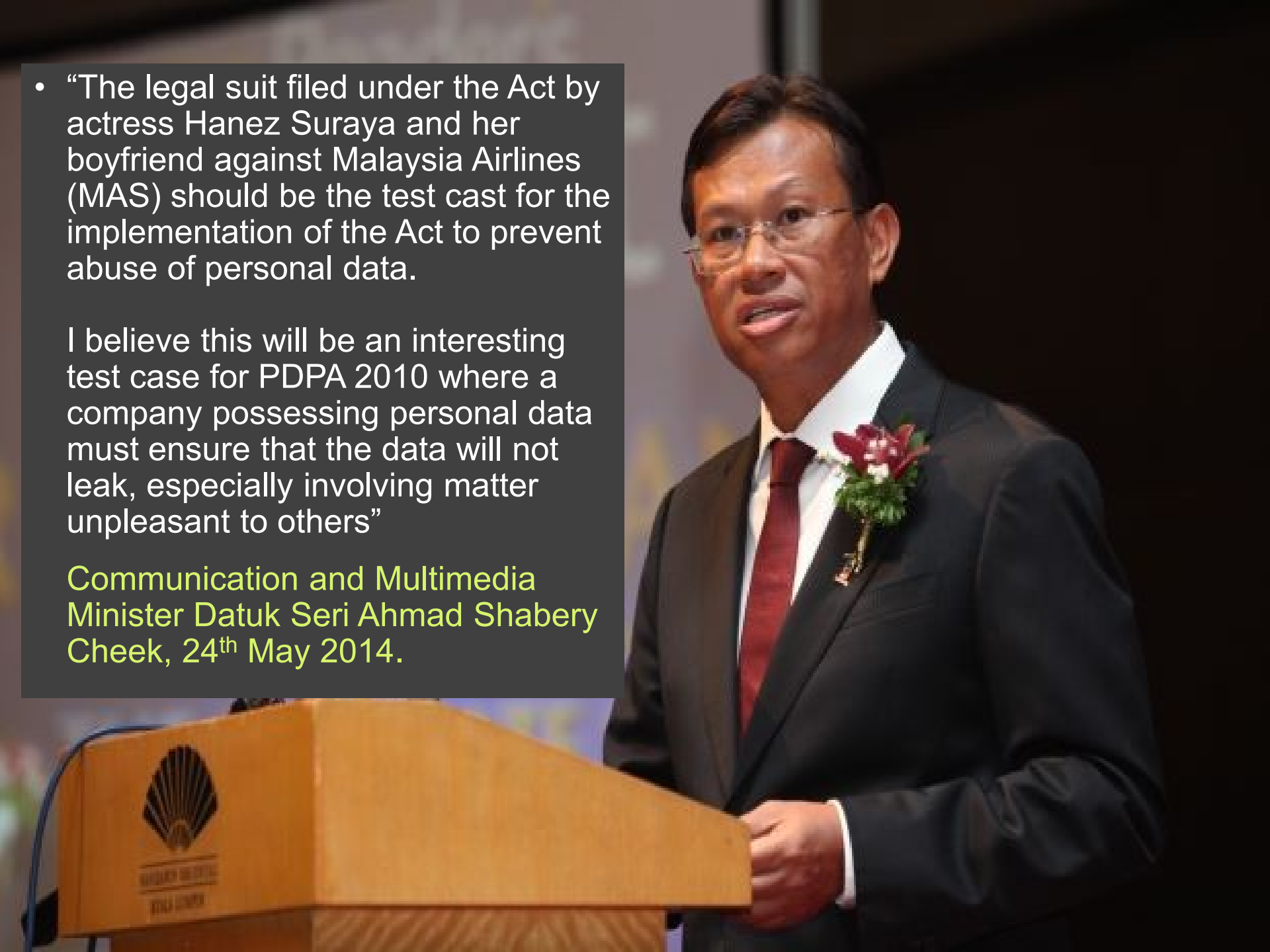
JOHOR: Court held an installation of **CCTV** directed towards other's house entrance as a breach to privacy (2011)

Hanez Suraya, kekasih saman MAS dedah maklumat tiket

Shah Alam: Pelakon Hanez Suraya Abdul Aziz (**gambar**) dan teman lelakinya memfailkan saman terhadap Penerbangan Malaysia (MAS), kerana mendedahkan mak-

ABPBH perin kehilangan M

» Kemunculan Liza Hanim, Nora diangka



- “The legal suit filed under the Act by actress Hanez Suraya and her boyfriend against Malaysia Airlines (MAS) should be the test cast for the implementation of the Act to prevent abuse of personal data.

  I believe this will be an interesting test case for PDPA 2010 where a company possessing personal data must ensure that the data will not leak, especially involving matter unpleasant to others”

  Communication and Multimedia Minister Datuk Seri Ahmad Shabery Cheek, 24th May 2014.

KEY FEATURES UNDER PDPA 2010

- Scope & Applicability
- Key Definitions
- PDP Principles
- Rights of Data Subjects
- Offences
- Governance & Enforcement

ClipartOf.com/1047013

The Objective and Scope of PDPA 2010

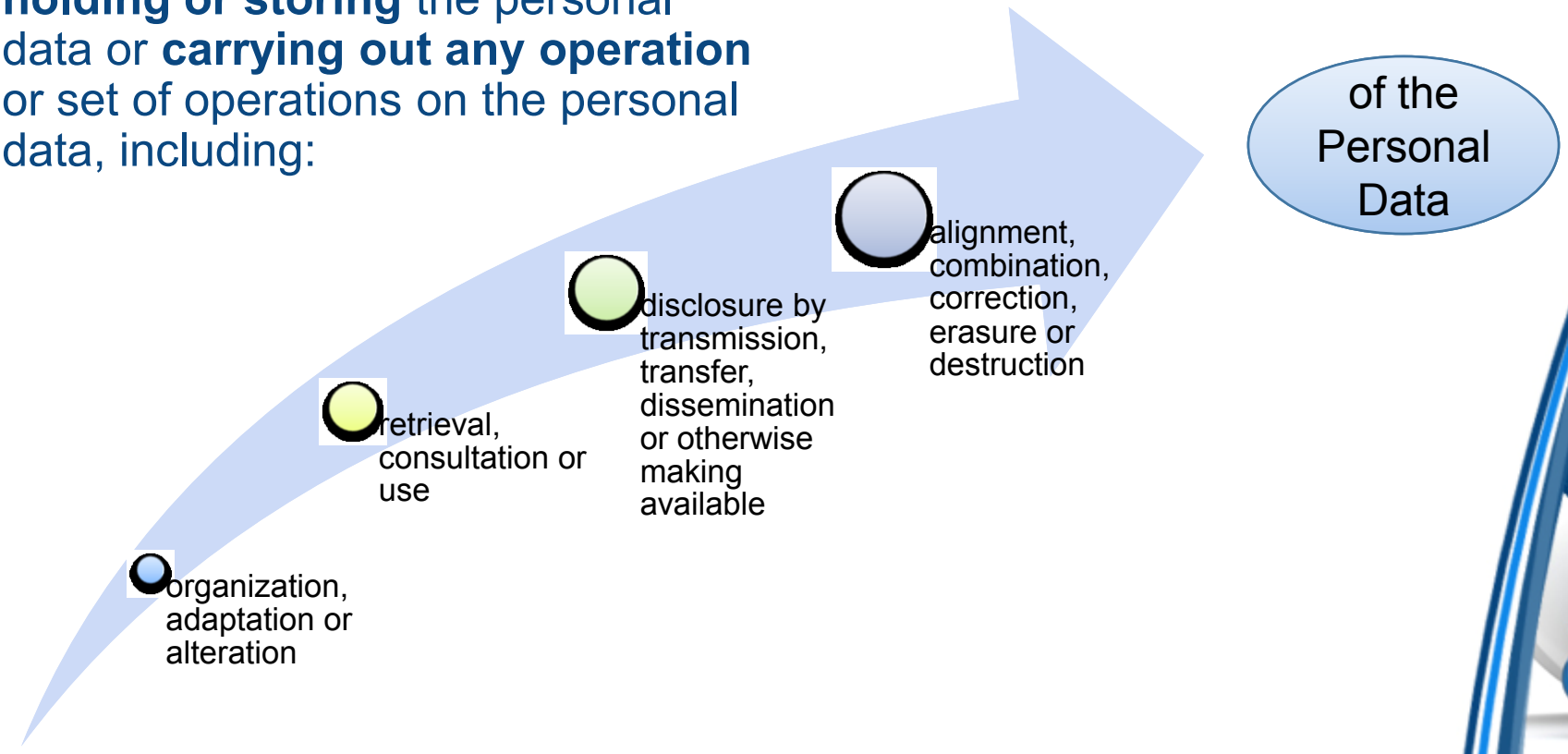
- To regulate the processing of personal data in commercial transactions and matters connected thereto.

- The Act applies to any **person** who:

processes **OR** controls or authorizes the **processing** of any **personal data** in respect of **commercial transactions**.

“Processing”

Processing, in relation to personal data, means **collecting, recording, holding or storing** the personal data or **carrying out any operation** or set of operations on the personal data, including:



“Personal Data” is any information:

in respect of **commercial transaction**;	• any transaction of a commercial nature, whether contractual or not *(includes goods, services, agency, employment, etc)*
that relates directly or indirectly to a **data subject**	• an individual who is the subject of the personal data *(regardless nationality/residence)*
Where that data subject is identified or identifiable	• from that information alone or from that and other information in data user’s possession
including any **sensitive** personal data	• On his physical/mental health/condition, his political opinions, religious beliefs, the (alleged) commission of any offence
Including **expression of opinion** about the data subject	• *e.g. data user’s opinion his former employee*
Processed by **automated** means OR is recorded as part of **relevant filing system**	• *Thus it applies to both electronically processed data and paper-based document*

Personal Data in a University

Intellectual Property

Communications Data

Union & Political Membership

Employment history

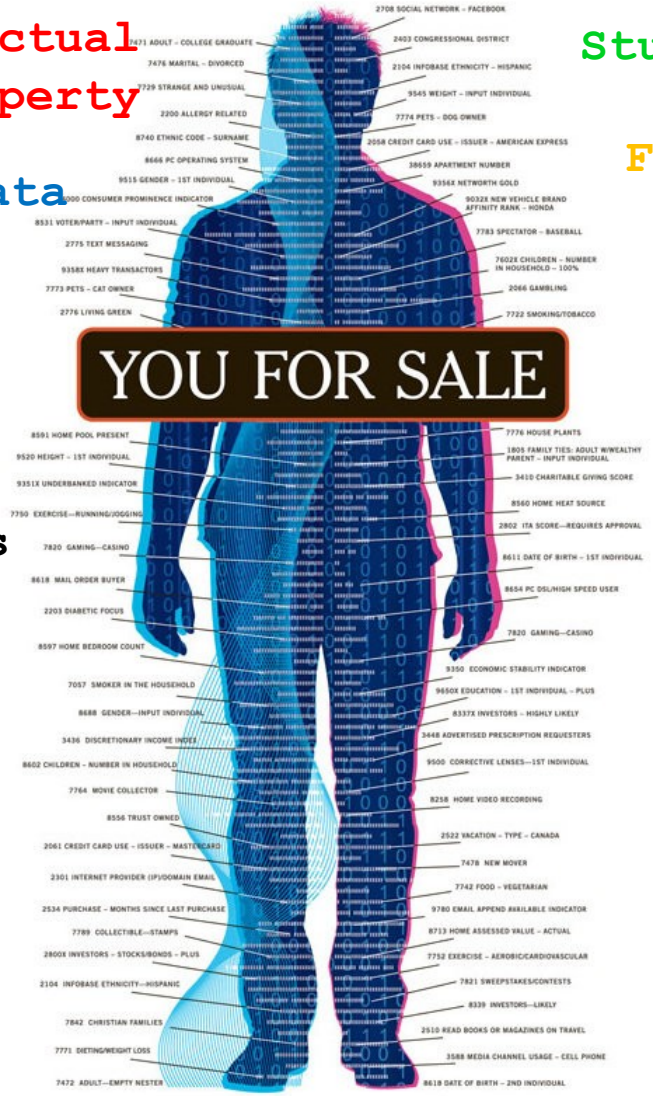
Immigration matters

Credit History

Transactional Information

Travels

Previous convictions



Pic: http://willscullypower.wordpress.com

Students records

Family background

Health Records

Disciplinary files

Scholarship

Citizen ID

Extra Curricular

Insurance Record

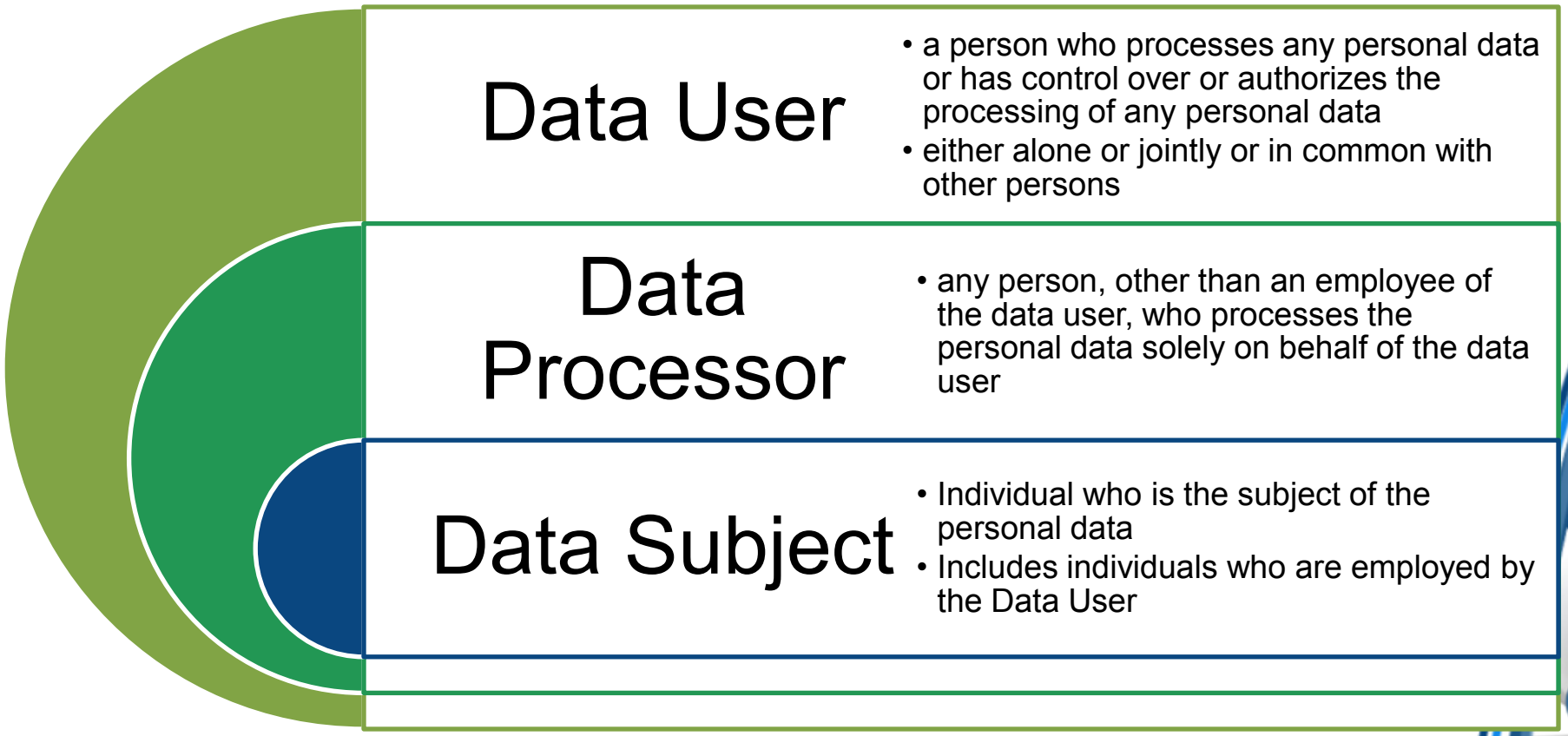
Social Networking

What is Not Protected?

WHAT IS NOT PROTECTED BY PDPA 2010

- Data processed by Federal & State Government
- Data solely & wholly processed outside Malaysia
- Data processed in non-commercial transactions
- Data processed for credit reporting business
- Data processed by an individual only for the purposes of that individual's personal, family or household affairs

The “Cast”



Personal Data Ecosystem

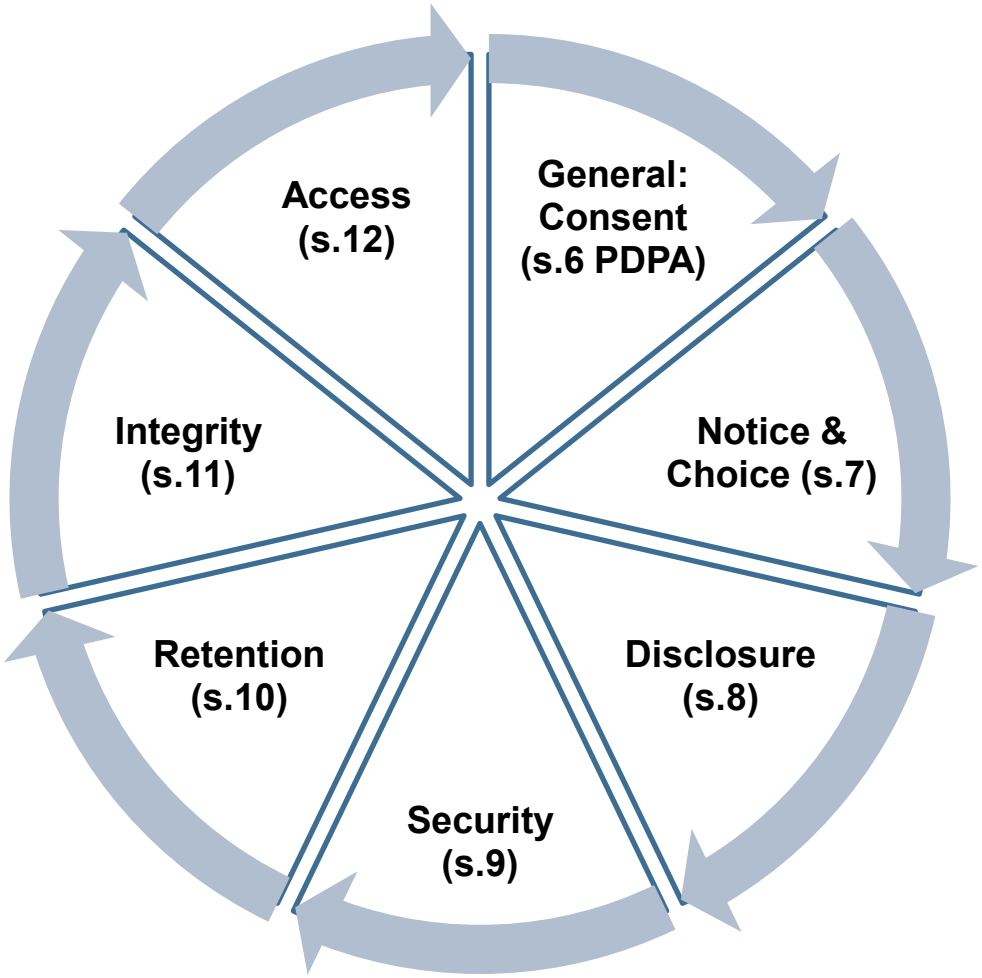
BOARD, SENATE & MANAGEMENT

EMPLOYEES

BUSINESS PARTNERS, SERVICE PROVIDERS

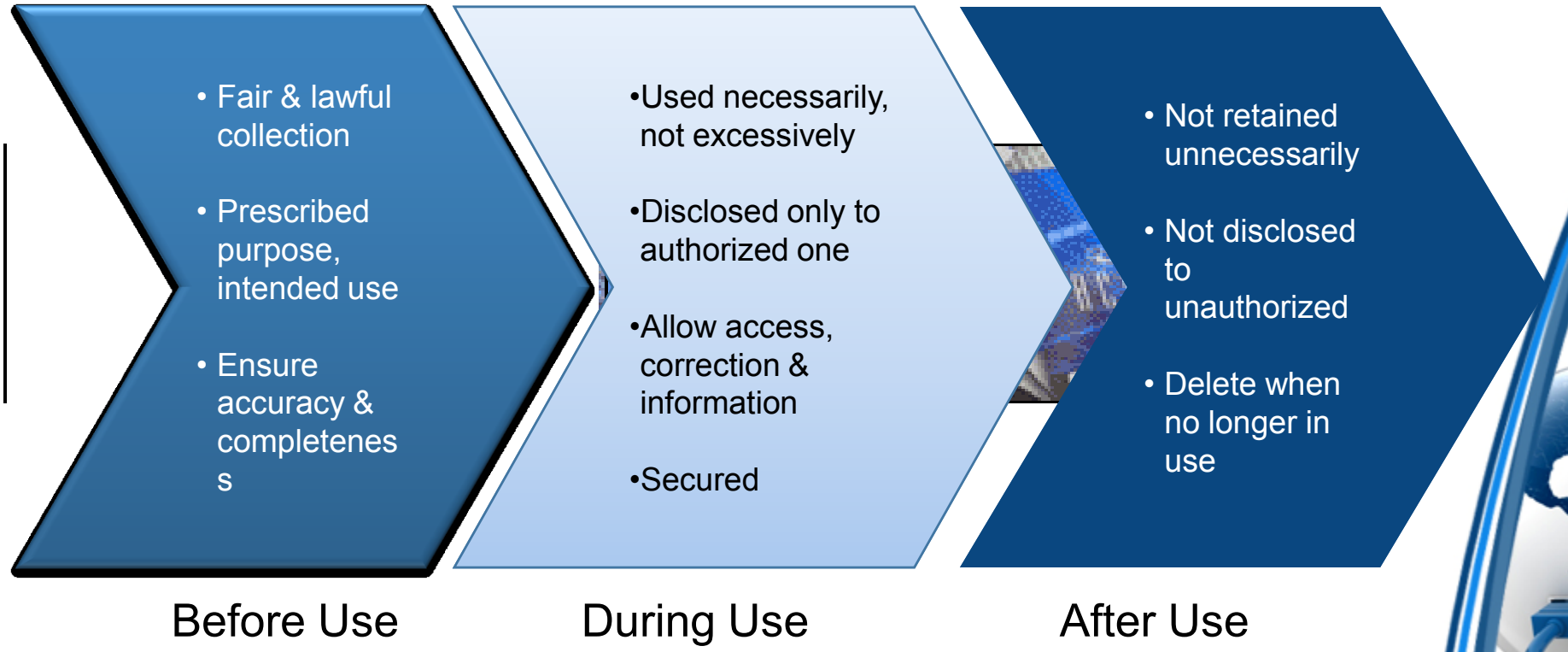
STUDENTS, PROSPECTIVE STUDENTS, ALUMNI

Seven PDP Principles

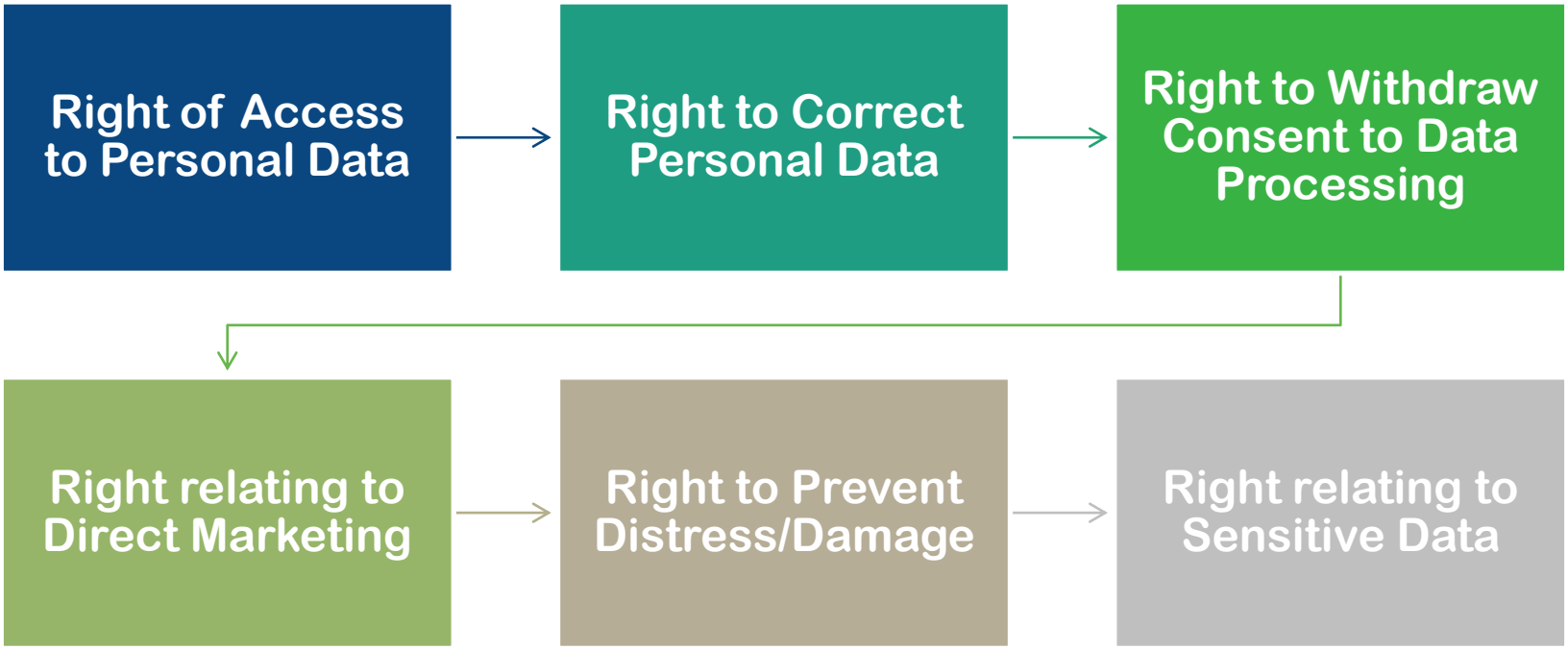


Data user who contravenes the above Principles commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

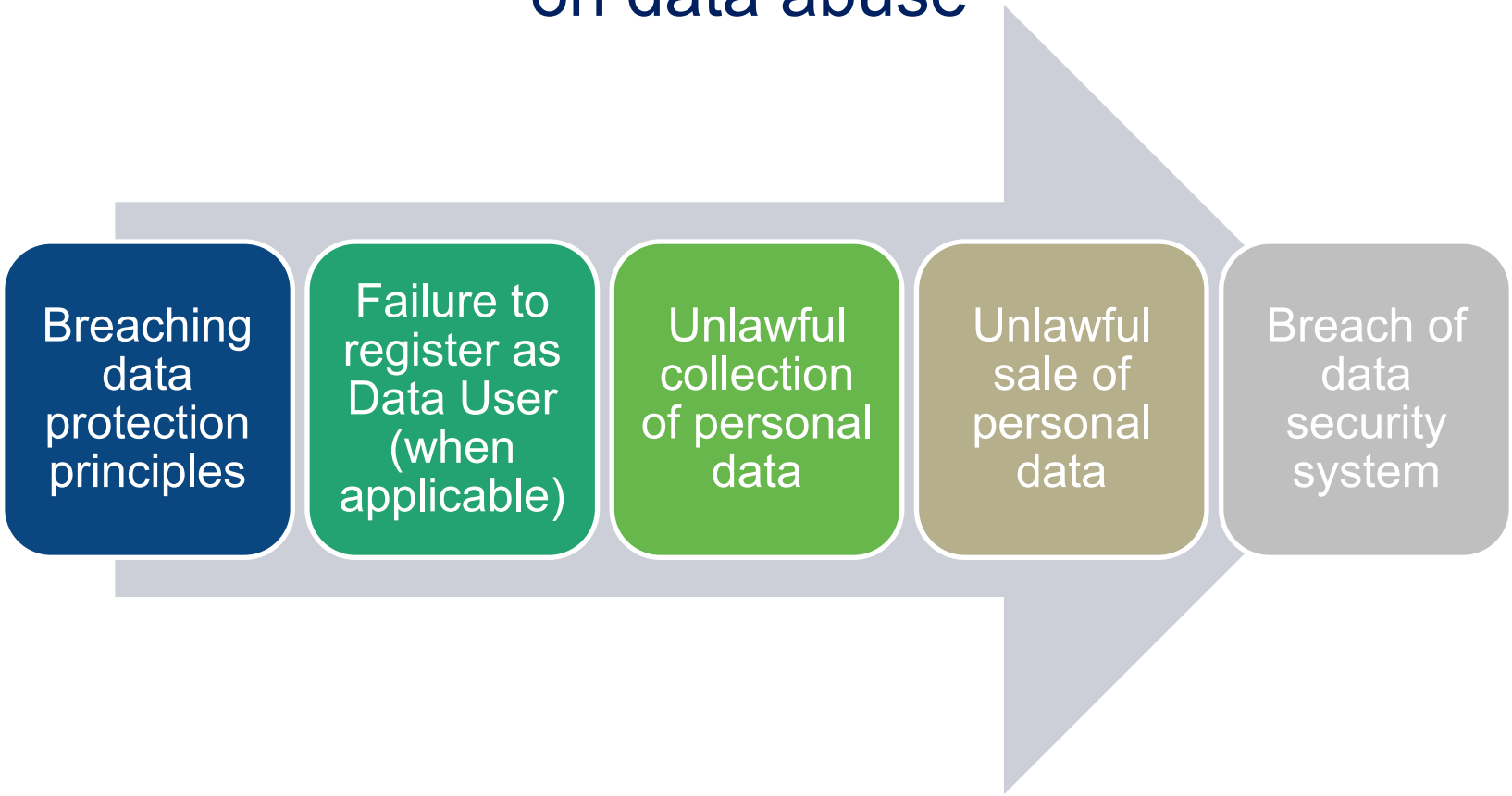
PDP Principles throughout the Personal Data Lifecycle



Rights of Data Subjects

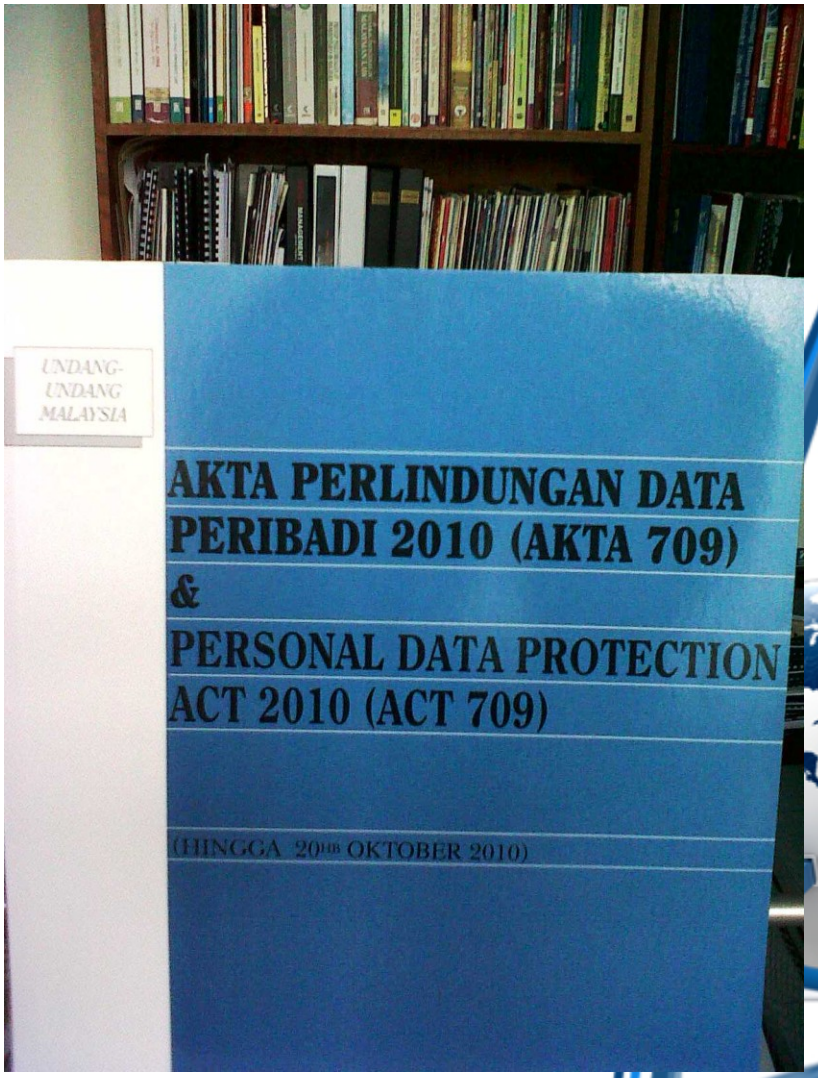


PDPA 2010 creates new offences on data abuse



Current status…

- PDPA has been in force since 15th November 2013
- Establishment of **Personal Data Protection Department** (JPDP) under the Ministry of Communications and Multimedia (MCMM)
- Appointment of the **PDP Commissioner**
- Relevant **subsidiary rules**
  1. PDP Regulations 2013 [P.U. (A) 335]
  2. PDP (Class of Data Users) Order 2013 [P.U. (A) 336]
  3. PDP (Registration of Data User) Regulations 2013 (P.U. (A) 337)
  4. PDP (Fees) Regulations 2013 (P.U. (A) 338)
- In the **pipeline**…
  - Guideline on Direct Marketing



CLASSES OF DATA USERS

[Gazetted under PDP (Class of Data Users) Order 2013]

Communications	Banking & Financial Institution	Insurance	Health
Tourism and Hospitalities	Transportation	Education	Direct Selling
Services	Real Estate	Utilities	

A data user who belongs to two or more classes of data users shall make a separate application for registration – PDP (Registration of Data Users) Regulations 2013.

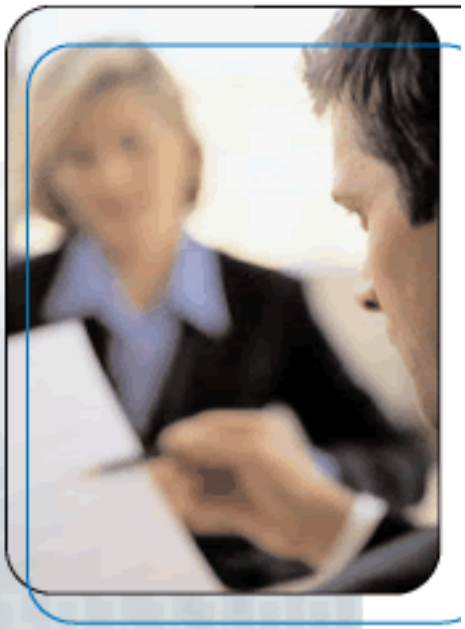
Compliance with Standards of Personal Data Protection [PDP Regulations 2013 [P.U. (A) 335]

- The Regulations provides the basis for “standards”.

- “Standard” means a **minimum requirement** issued by the Commissioner, that provides, for common and repeated use, rules, guidelines or characteristics for activities of their results, aimed at the achievement of the optimum degree of order in a given context.

- Several standards to come:
  - Security standard
  - Retention standard
  - Data integrity standard

Compliance with Inspection Requirements
[PDP Regulations 2013 [P.U. (A) 335]



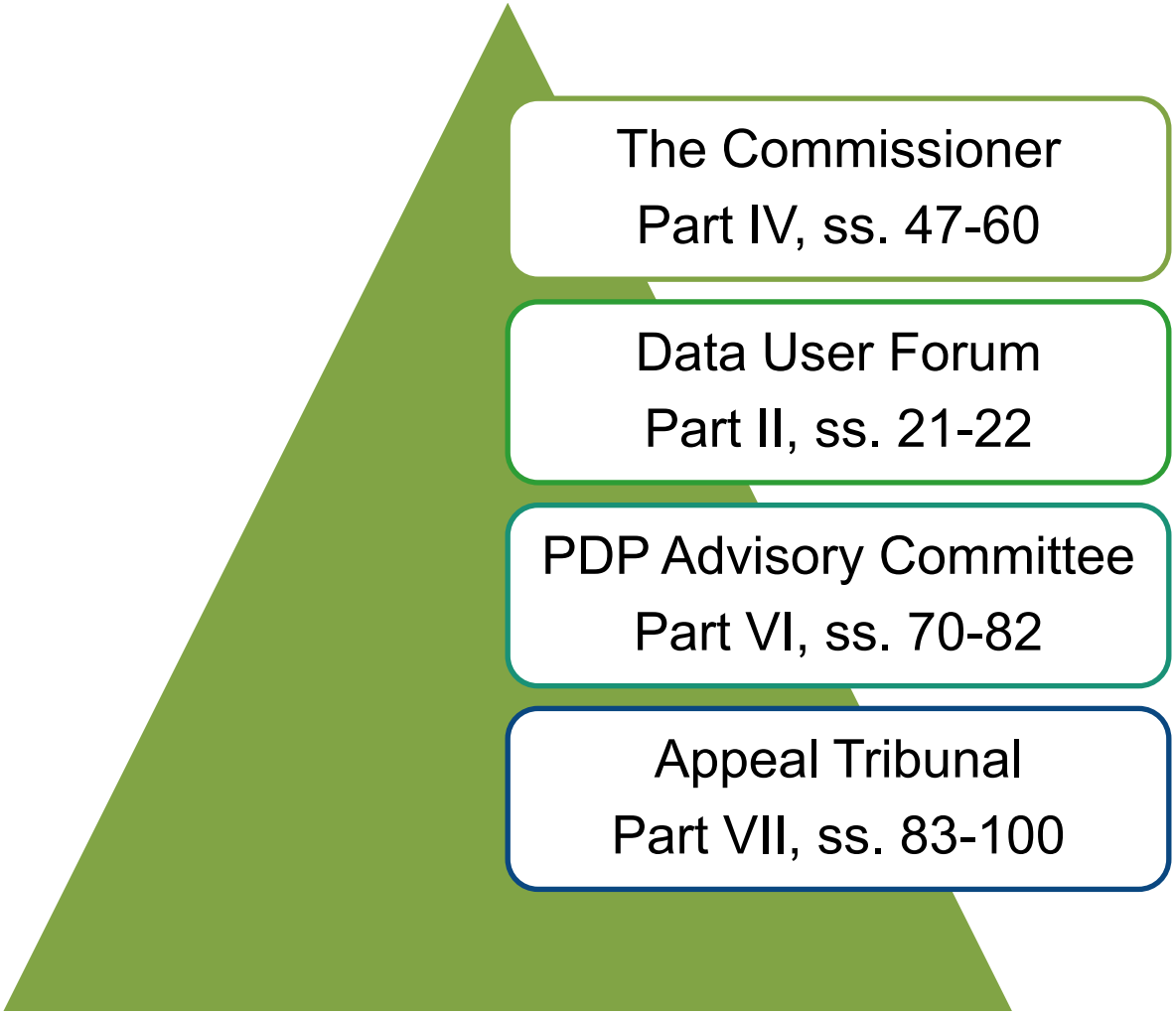
- Inspection of Data system would require the production of the following:
  - ❑ Record of the data subject's consent to the processing
  - ❑ Record of written notice to data subject ("Collection Notification")
  - ❑ List of third party disclosure
  - ❑ Security policy
  - ❑ Record of compliance with retention standard
  - ❑ Record of compliance with data integrity standard
  - ❑ Any other information, e.g. engagement with data processors

Complaint & Enforcement

Section 104

- Any individual or relevant person may make a complaint to the Commissioner of any potential contravention of the Act or Codes of Practices.
- The complaint must be made in writing.
- Upon investigation, the Commissioner may serve on the relevant data user an **enforcement notice** before serving any penalties or proceeding with prosecution.
- An appeal is allowed to be brought by any person who is aggrieved by decision of the Commissioner

The “Governance”



PDP Law in University – What does it mean to you and me?

- For the University

  As a data user: Have they adopted the PDP Principles in their business process? Have they inculcated the data privacy and security culture? Have they taken steps to manage the risks in relation to data protection? Have they come up with comprehensive governance and compliance framework?

- For the staff/employee

  Are you aware of the data ecosystem in the University? As “agent” of data user, are you aware of the implication of PDP Act to your work? As data subject (being employee) are you aware of your personal data rights?

- For the students

  Are you aware what personal information you have submitted to the University and for what purpose? Are you aware of your rights to your personal data as students and/or alumni?

THANK YOU

sonny@iium.edu.my

http://sonnyzulhuda.com